Transferring a configuration file from one model to another

Transferring a configuration file from one FortiGate model to another

*** IS NOT SUPPORTED BY FORTINET ***

However, there are some circumstances where the replacement for a FortiGate is not the same model and the configuration is complex enough that you will want to give it a try. 99.9 % of the time it is not possible to seamlessly use a configuration file from one model on another but because the configuration file is a text file to be read by the firmware each time the unit boots up it is theoretically possible to use another model's configuration file as the basis for the configuration of a different model. The file needs to be edited, sometimes extensively, preferably by someone comfortable with the syntax of these configuration files.

For those brave enough to attempt this sort of thing the usual approach is as follows:

1. Install a fresh copy of the firmware on the new device. The firmware has to be the exact same version as the one that was used to back up the configuration of the source device.
2. Execute factoryreset to verify that there is a clean configuration file.
3. Set up the Interfaces and modes as close as possible to the source device, using the same names and addresses.
4. Use the backup copy of the source device to cut and paste sections into the destination device through the Command Line Interface. The CLI will check for syntax errors as the commands are entered.
5. Run a diagnostic error check to see if there are any errors

The reality is that unless you are very knowledgeable and comfortable playing in the configuration file, it is easier and faster to build the new configuration from the ground up.

Useful Tools:

TFTP Server:

The following is a link to a free windows software utility that will perform the function of TFTP Server.

Tftpd32:

http://tftpd32.jounin.net/tftpd32_download.html

If it does not appear to work, the first step is to make sure that some other service or application is not using port 69.

Whenever using the TFTP server it is also important to turn off any software firewalls running on the computer acting as the server.

SSH/Telnet client

A commonly used client is Putty.exe. Download from:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Text Editor

Notepad++ can be downloaded for free from http://notepad-plus-plus.org/

The beauty of a source code editor like Notepad++ rather than Notepad is that it shows the indents in the code which will make things much easier and intuitive.

File Comparison software

Winmerge can be downloaded for free from http://winmerge.org/downloads/

If after the warnings and caveats you are still determined to try, the procedure follows...

On the Original Device

Step # 1 - Verify that you have a working configuration that performs its functions properly.

Step # 2 - Verify the Version, the MR level, the Patch Level and the build number of the firmware of the original device.

- Using the top line of the Configuration file:

  If you can read the top line of the configuration file with a code editor or even a text editor, you will get a line similar to the one in this example:

```
#config-version=FGT60C-4.00-FW-build328-
110715:opmode=0:vdom=0:user=admin
```

Right after the model number, "FGT60C-" is the version number, in this case 4.00. We now know the version number. The build number can be used to narrow it down to a MR number and patch number.

- Using the Web Based Interface:

  In version 4.3.x

  Goto System → Dashboard → System Information Widget

  Line: "Firmware Version" - should be something similar to v4.0,build0656,130211 (MR3 Patch 12) [Update] [Details]

- The Command Line Interface:

  Run the command: `get system status`

  There are more lines of output than are seen here but the relevant ones are:

  - In Version 4 MR 2 and earlier:

    ```
    Version: Fortigate-60C v4.0,build5840,110715 (MR2)
    Branch point: 328
    Release Version Information: MR2
    ```

  - In Version 4 MR 3 and later:

    ```
    Version: FortiWiFi-80CM v4.0,build0458,110627 (MR3
    Patch 1)
    Branch point: 458
    Release Version Information: MR3 Patch 1
    ```

  The difference being that starting in MR3, the patch number is included as well as the MR version and the build number is consistent with the branch point.

  If you need to know which Branch point corresponds with which Firmware image you can:

  - Check the Upgrade Path document at http://docs.fortinet.com/fgt/FortiOS-Upgradepath.pdf
  - Log into a Support Chat session and ask the tech on duty.

Step # 3 - Backup the working configuration file

There are a number of ways but the simplest is through the Web Based Manager.

Go to System → Dashboard → Status → System Information Widget

Go to the line: System Configuration

Click on [Backup]

Save the file to your local PC

On the New Device

Step # 4 - Install the same firmware on the device as is on the original device.

Upgrades can be done afterwards but during the transition, in order to minimise the possibility of syntax errors it is important that the devices match in terms of firmware. If the new device came from the factory with a more recent version of the firmware there are 2 options:

1. Upgrade the original device to the same level as the new device or

2. Install the same version being used by the original device on the new device using a console cable and a TFTP server.

Process for installing firmware via console cable:

Ideally, you want to do this using a console cable, a SSH/Telnet client and a TFTP server

1. Connect the Console cable

   Using the console cable, connect the computer running the TFTP server to the FortiGate unit.

2. Connect Ethernet Cable

   Connect an Ethernet cable from the Fortinet Device to either the computer or a network that is on the same subnet as the computer hosting the TFTP server. The port on the Fortinet device that you would connect the Ethernet cable to is usually the Internal port 1.

3. Log in to the Fortinet device with your SSH/Telnet client.

   Connect to the device using the following settings:

Speed:	9600
Data bits:	8
Parity:	N
Stop bits:	1
Flow Control:	No Hardware Flow Control

4. Reboot / power cycle the Fortinet Device and bring up the menu

   As the console displays text as it boots up, it will eventually display the line

"Press any key to display configuration menu..."

Press the spacebar or any other key.

5. Format the boot device

   If the menu includes `Format boot device [F]` press F and wait for the device formatting to complete.

6. Download the firmware

   Press `G` to start firmware download.

   The console displays:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

   Type the IP address of the computer running the TFTP server and press Enter.

   The console displays:

   ```
   Enter Local Address [192.168.1.188]:
   ```

   Type an unused IP address that is on the same subnet as the TFTP server and press Enter.

   The console displays:

   ```
   Enter File Name [image.out]:
   ```

   Type the firmware image file name and press Enter.

   The console periodically displays a "#" (pound or hash symbol) to show the download progress.

   When the download completes, the console displays a message similar to:

   ```
   Save as Default firmware/Run image without
   saving: [D/R] Press D.
   ```

The FortiGate unit installs the new firmware image and restarts. The installation may take a few minutes to complete.

Step # 5 - Set to factory Default

This will clear away all previous settings and configurations

Using the command line interface submit the command:

```
execute factoryreset
```

Once this is finished you should have a clean, default configuration file installed on your new device

Step # 6 - Set up the interfaces of the new device as closely as possible to match the original devices.

- To log into the clean system you will likely use the default IP address of 192.168.1.99 on the Internal ports.
- Make sure the mode of the internal ports matches, i.e. Interface mode, switch mode, or hub mode.
- Make sure the names of the interface match.
- Make sure that the IP addresses used on the Interfaces.
- Make sure that any DHCP Servers or DNS servers match.

Step # 7 - Add configuration components to the baseline configuration.

This section should be prefaced with the warning that you should not copy over anything that relates directly to the configuration of the interfaces as you could "break" the device if the configuration does not match the hardware. In terms of best practices you should also only copy and paste sections of the configuration where you understand the purpose of the lines of code that you are moving over at least in a general sense.

You will need a text editor or a source code editor that can read the configuration file in a user-friendly fashion.

I like using Notepad++, but it is always best to use what you are comfortable with.

You will probably also want a SSH client to connect to the Fortigate with rather than use the widget in the Dashboard window. It is possible to use the widget but using a separate client will allow you to expand the window so that you aren't feeling cramped on the screen. Putty is a commonly used client.

Rather than using the GUI to go through all of the steps or typing in all of the commands through the CLI we are going to copy from the configuration file as displayed in the source code editor and paste it into the CLI.

The CLI will catch any syntax errors and most logical errors.

You should be able to copy and paste in sections, saving a lot of time. The thing to remember is to do it in the correct sections. The code editor should show the lines of the configuration with indents from the left depending on how nested the cli command is. You want to copy entire nested section that can be entered from the "root" command prompt. In other words, from a line that has no indent to the next line that has no indent. For instance in the example below you would copy and paste the entire group from the line starting with "config" to the line containing "end". The command structure of the CLI is context sensitive. If you tried to copy from the line starting with "edit" we would have to first manually enter the command "config system accprofile", otherwise you would get errors.

```
config system accprofile
     edit "prof_admin"
```

```
                set admingrp read-write
                set authgrp read-write
                set endpoint-control-grp read-write
                set fwgrp read-write
                set loggrp read-write
                set mntgrp read-write
                set netgrp read-write
                set routegrp read-write
                set sysgrp read-write
                set updategrp read-write
                set utmgrp read-write
                set vpngrp read-write
            next
        end
```

The copying from the source code editor is straight forward enough, select the text you want to copy and right click | select copy or use the hot keys CTRL+C. To paste into the CLI with Putty, just make sure that you are already logged in through Putty and that you are at the "root" prompt, use the left mouse button to select the Putty window and then right click anywhere within the window. This will paste the commands in the right order into the CLI. If you get any errors the CLI will immediate give you error messages and you can deal with them right there where you know the error is occurring. This is why we want to do the copying is discrete batches.

For those that are more familiar with the configuration you may want to skip sections that are likely to be common to all configurations such as the replacement messages.

Continue copying and pasting until you reach and end of the configuration file.

Step # 8 - Make a copy (backup) of the current configuration file.

Step # 9 - Test to make sure the unit is operating as desired

Step # 10 - Compare original configuration file to the current one for differences. (Optional)

Use a product like Winmerge to make the comparison of the files easier. The files will never be completely the same but by running the comparison, you can check for obviously missing sections and differences.

Troubleshooting:

After you have completed entering the configuration settings you can do a final check of the configuration by running from the command line interface:

```
diagnose debug config-error-log read
```

If there are any configuration issues in the new file this command will give as an output the line where the configuration stops working according to its diagnostic rules.